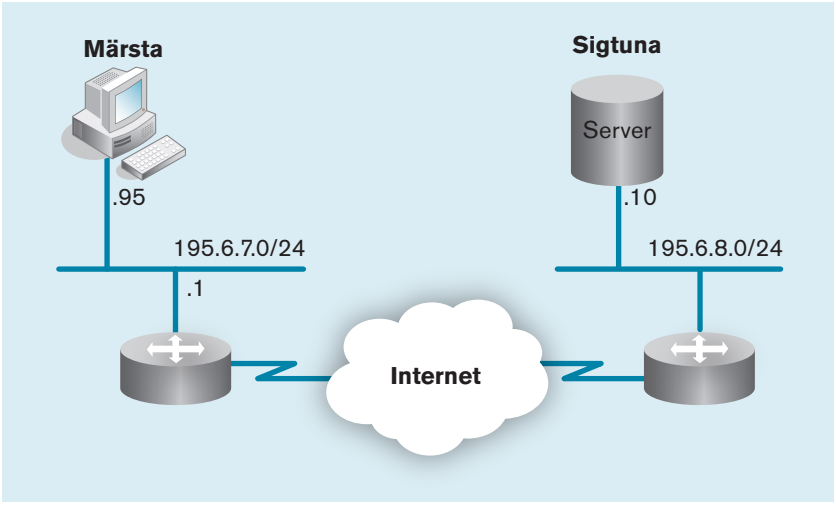
Felsökning i TCP/IP-miljö

- I detta kapitel går vi igenom felsökning på IP-nivå med hjälp av ping och traceroute. De funktioner som är inblandade i routing och namnuppslagning gås igenom samt hur man kan fastställa var i kedjan felet ligger. Felsökning av webb och e-post gås igenom kortfattat.
- Kapitlet kan läsas fristående.

Om vi tänker oss följande nätverk där en klient i Märsta ska nå en server i Sigtuna så finns det en massa komponenter och program som måste fungera. Servern och klienten måste självklart fungera, men även alla routrar till och från servern, namnuppslagning samt normalt även ett par brandväggar.

Grundläggande felsökning är att prova från en annan klient i Märstanätet. Eller att prova om man från klienten kan nå en annan server. En annan åtgärd är att undersöka länk-indikatorn på Ethernet, om den inte lyser finns ett fel på Ethernet-nivå. Men vi ska i detta läge utgå från IP-nivån.



Nätskiss hur IP-klienten i Märsta når servern i Sigtuna

Vi börjar med att ta reda på den konfiguration som gäller med kommandot ”ipconfig /all” i Windows, ”ifconfig -a” i Unix. Vi kan då kontrollera att standard gateway går att nå, observera dock att DNS inte behöver ligga på samma subnät.

Använd ipconfig eller ifconfig och kontrollera att routern kan nås. Fel på IP-nivån är ofta rena felkonfigurationer. Vi avsåg att mata in 195.6.7.95 men det blev 195.6.79.5 eller något liknande. Ett annat problem är vanan att alltid ställa masken till 255.255.255.0, det behöver inte alltid stämma.

```
Ethernet-kort Local Area Connection:

        Anslutningsspecifika DNS-suffix . . :
        Beskrivning . . . . . . . . . . . . : Intel(R) LAN 2435
        Fysisk adress . . . . . . . . . . . : 00-13-CE-26-F9-18
        DHCP aktiverat  . . . . . . . . . . : Nej
        Autokonfiguration aktiverat  . . . . : Nej
        IP-adress . . . . . . . . . . . . . : 195.6.7.95
        Nätmask . . . . . . . . . . . . . . : 255.255.255.0
        Standard-gateway  . . . . . . . . . : 195.6.7.1
        DNS-servrar . . . . . . . . . . . . : 195.6.17.2
```

Börja med att kontrollera IP-konfigurationen.

Ipconfig-kommandot med tillägget /all ger dessutom information ifall DHCP används eller inte. Eftersom många nätverk använder samma privata IP-adressrymd är det lätt att komma från ett nätverk med nästan rätt konfiguration till ett annat. Bara ipconfig visar rätt resultat, IP-adresserna är samma i bägge nätverken. Med tillägget /all kan vi till exempel se om vi har rätt DNS och hur aktuellt DHCP-lånet är.

Det enklaste sättet att felsöka vidare är sedan att pinga sig ut. Vi börjar med vår egen adress (localhost), sedan pingar vi den normala adressen. Nästa steg är att pinga standard gateway (eller en annan nod på det lokala nätverket), namnservern och sist den server vi vill nå.

Exempel på hur du kan pinga dig ut, från localhost, via standard gateway till rätt server.

```
Ping 127.0.0.1
Ping 195.6.7.95
Ping 195.6.7.1
Ping 195.6.17.2
Ping 195.6.8.10 alt. ping www.server.se
```

I en mening är ping trivialt, men de mekanismer som krävs för att ping ska lyckas är inte triviala. Routing mellan klient och server måste fungera bägge vägarna. Det kan mycket väl vara så att klienten hittar till servern. Men när servern ska tillbaka till din klient har Märsta-nätet gjort ändringar som de inte meddelat sin Internetoperatör. Därför är nätet inte känt hos operatören så paketet kommer inte fram.

Även arp-kommandot kan var användbart. I bilden ovan ska arp-cahchen innehålla MAC-adressen för standard gateway. Använd kommandot ”arp -a”.

Ett annat sätt att felsöka är att utgå från vilka portar som är öppna, vilket vi kan kontrollera med kommandot ”netstat -an”. Detta är väldigt användbart på servrar. Aktuell port ska vara öppen och status på processen är vanligtvis ”listening”. Om en process gått igång och är i status listening men den externa adressen är 127.0.0.1 så accepterar servern bara inkommande förfrågningar från den egna maskinen. Kontrollera i så fall konfigurationsfilen.

Kommandot netstat -a kan även ge dig information om du tror att du har fått virus. Ett virus (eller en så kallad zoombie) kan ligga och vänta på en port. När någon sedan kopplar sig mot din dator kan han/hon använda den för egna syften.

```
Aktiva anslutningar

  Prot.  Lokal adress            Extern adress          Status
  TCP    0.0.0.0:80              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5225            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5226            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8008            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1026          127.0.0.1:5225         CLOSE_WAIT
  TCP    127.0.0.1:1042          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1115          127.0.0.1:5225         CLOSE_WAIT
  TCP    127.0.0.1:1119          127.0.0.1:5225         CLOSE_WAIT
  TCP    127.0.0.1:5226          127.0.0.1:1030         ESTABLISHED
  TCP    127.0.0.1:5679          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8005          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:10110         0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445             *:*
  UDP    0.0.0.0:500             *:*
  UDP    0.0.0.0:4500            *:*
  UDP    127.0.0.1:123           *:*
  UDP    127.0.0.1:1900          *:*
```

Etablerade sessioner visas som ”established”. På klientsidan har vi inte kontroll på vilken port som används men vi kan se på den externa adressens port om det stämmer.

Ungefär år 2003 inträffade också en stor förändring i både Windows- och Unix-miljöer. Alla produkter levereras med olika typer av personliga brandväggar. Ibland fungerar det automatiskt men flera produkter har problem, även om man sätter igång serverprodukten så är brandväggen stängd. Även ICMP och specifikt ICMP echo är oftast avstängt som förvalt värde. Säkerheten ökar men felsökning blir komplexare.

Kontrollera att den interna (personliga) brandväggen är rätt inställd och öppen på rätt portnummer.

Namnservern

Alla protokoll inom Internetsviten klarar att användas med IP-adresser eller nodnamn. ”Ping www.sunet.se” eller ”ping 130.239.8.25” ska ge samma resultat. Ett enkelt sätt att kontrollera namnuppslagning blir alltså att pinga ett nodnamn och se att namnuppslagning fungerar.

```
C:\>ping www.sunet.se

Skickar signaler till www.sunet.se [130.239.8.25] med 32 byte data:

Begäran gjorde timeout.
Begäran gjorde timeout.
Begäran gjorde timeout.
Begäran gjorde timeout.

Ping-statistik för 130.239.8.25:
    Paket: Skickade = 4, mottagna = 0, Förlorade = 4 (100 %),
```

Namnuppslagningen ser ut att fungera, vi ser att den försöker kontakta 130.239.8.25. Vill man göra en ytterligare kontroll kan man använda kommandot nslookup. Ur resultatet nedan kan vi se två saker förutom själva svaret på namnfrågan. Vi kan se vilken namnserver som levererat svaret (ns.local.teliamobile.net nedan) och vi kan se att svaret är mellanlagrat och inte har verifierats av den server som är ansvarig för domänen (det står att svaret är ”Non-authoritative”). Eftersom DNS bygger på mellanlagring finns ett problem när information ändras, det tar tid innan ändringen slår igenom.

```
C:\>nslookup www.sunet.se
Server:  ns1.local.teliamobile.net
Address:  10.0.0.1

Non-authoritative answer:
Name:    www.sunet.se
Address:  130.239.8.25
```

För att kunna göra dig oberoende av fel information i DNS behöver du ett par saker och dessa bör du skaffa dig innan DNS fungerar dåligt. Dels bör du kunna IP-adresser till ett par servrar på Internet, eller centralt på företagsnätet. så du kan hoppa över namnuppslagningstjänsten.

Om du misstänker problem med din namnserver kan du med nslookup eller kommandot dig ställa frågan till en annan namnserver. Leta därför upp en namnserver på Internet som tillåter rekursiva frågor, eller använd en webbsida som tillåter nslookup- eller dig-frågor.

När PING inte går att använda

Tyvärr svarar inte alla noder och nätverk på ping. Organisationer kan ha stängt av ICMP echo eller till och med all ICMP trafik i brandväggar eller med hjälp av filter. Ett alternativ är då att använda programmet telnet, men att anropa den port som servern förväntas svara på. Sedan förväntas man använda rätt kommando för att servern ska svara, men även om man skriver ett felaktigt kommando så brukar man få svar (servern svarar med att kommandot inte finns eller att syntaxen är fel).

```
C:\>telnet www.firma.se 80
```

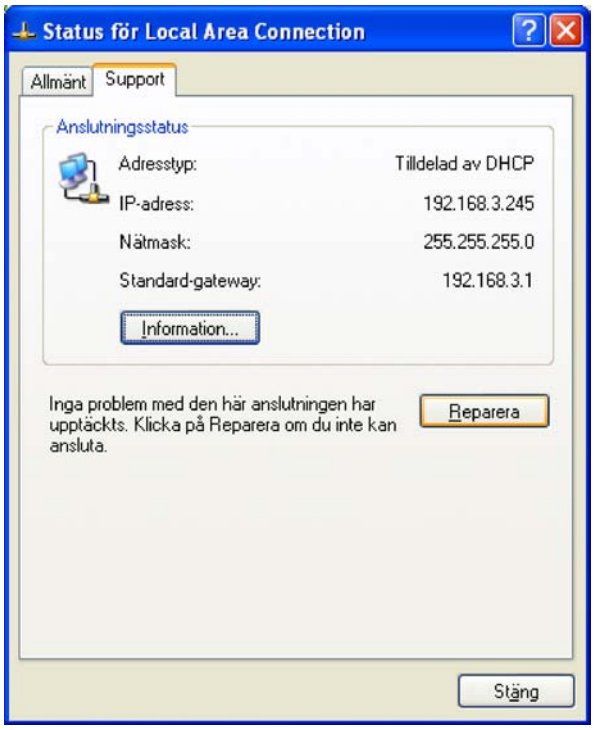
Grundläggande funktioner i HTTP, SMTP, POP-3, FTP är inte svåra att lära sig. Det är bara att öppna rätt RFC och läsa. HTTP version 1.1, MAPI, SIP med flera är svåra att hantera. Men även om vi får ett felmeddelande så tyder ju det på att paket kommer fram till servern och tillbaka. Och det är ju den information vi får via ping.

Fel i DHCP

Dynamisk tilldelning av IP-adresser via DHCP har drygt tio år på nacken och är beprövad teknik. De flesta DHCP-klienter fungerar stabilt idag. I Windows 2000 och XP service pack 2 lade Microsoft till funktioner för att automatiskt förnya DHCP-lån varje gång förändringar sker på länknivån (till exempel om vi byter från ett WLAN-nät till ett annat). En förändring som i sin enkelhet gör att DHCP fungerar ännu bättre.

Om man fortfarande misstänker problem med den adress datorn erhållit via DHCP så kan man ge kommandot ”ipconfig /release” följt av ”ipconfig /renew”. I Windows XP är det enklare, DHCP-lånet förnyas om man väljer att reparera nätverksanslutningen.

Vad ska en nod göra om den ställs in på att använda DHCP men inte får kontakt med en DHCP-server? Den skulle kunna låta bli att starta nätverkstjänsten.



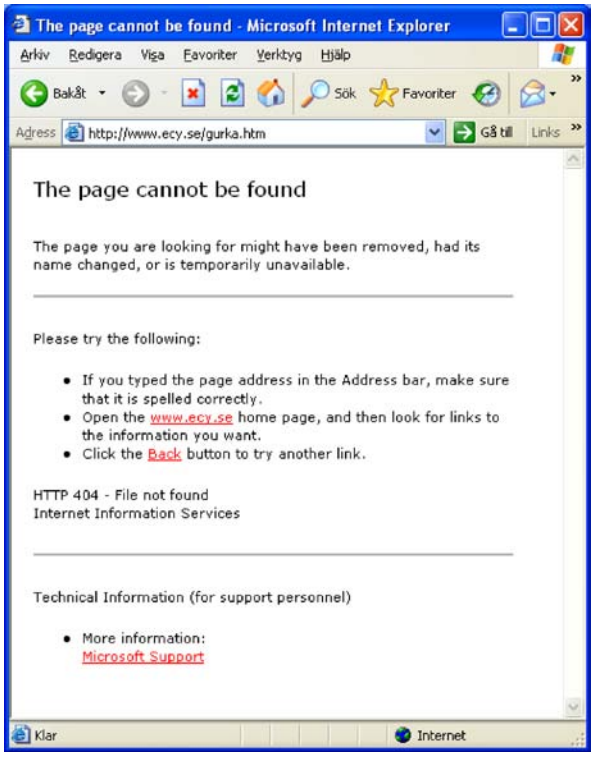
När anslutningen repareras förnyas även DHCP-lånet.

Om din maskin valt en IP-adress som börjar på 169.254. så tyder det på att den inte fått kontakt med en DHCP-server.

En annan lösning är att den tar en slumpgenererad adress ur adressrymden 169.254.0.0/16. Detta utrymme är reserverat för självkonfiguration. Microsoft kallar funktionen APIPA (Automatic Private IP Addressing), och den finns beskriven i tekniska dokument. Klienten tar en slumpartad adress och gör sedan en ARP-förfrågan för att kontrollera om någon annan maskin har denna adress. I så fall gör den ett nytt försök. Funktionen fungerar bra och gör att en ovan användare lätt kan få ett litet IP-nät att fungera internt då alla maskiner hamnar på samma subnät.

Webbservrar

Felsökning av webbservrar fungerar som vilken servertjänst som helst. Kontrollera med netstat -an att servern lyssnar på port 80. Använd ping och traceroute för att kontrollera att paketen kommer fram. De vanligaste felen är felaktiga URL:er och felaktiga namn. Om vi skriver in en sökväg, eller klickar på en länk, som motsvarar en fil som inte finns så svarar servern med felmeddelande 404. Fel 404 visar att servern och routingen dit fungerar. (Jag undviker att säga något om kvalitén på Microsofts söktjänst om man skriver in fel nodnamn i Internet Explorer.)



Fel 404 betyder att mycket fungerar. Servern är uppe och routingen dit fungerar.

De flesta webbsidor består ju av en mängd objekt. Var och en med sin egen sökväg. För att hämtning av webbsidor ska fungera effektivt och inte ge upphov till en mängd namnfrågor mellanlagras svaren. Men även misslyckade namnuppslagningar mellanlagras (så kallad negativ caching). Om du vet att det borde fungera så prova att stänga webbläsaren och öppna den på nytt en stund senare.

Webbservrar är relativt lättkonverserade via telnet. Plocka fram kommandoläget och skriv in ”telnet webserver 80” samt slå enter två gånger. Du ska erhålla ett tomt fönster där servern väntar på ditt HTTP-kommando. Prova med något liknande:

```
GET /
GET /index.htm
GET /index.html HTTP/1.0
```

Om du fick resultatet ”website not found” så prova med den modernare varianten av HTTP:

```
GET /index.html HTTP/1.1
host:  www.dinserver.se
```

Om det gick bra så får du en mängd HTML-kod som svar (utdrag nedan):

```
<li> <a hr
ef=”http://se.yahoo.com/”>Yahoo</a>, <a
href=”http://www.webcrawler.com/”>Webcrawler</a>, <a href=”http://www.altavista.com/
”>AltaVista</a>, <a href=”http://www.google.com/”>Google</a>,
<a href=”http://www.alltheweb.com/”>Alltheweb</a>
</
ul>
<HR>

This server is maintained by <A HREF=”MailTo:webmaster@sunet.se”>webmast
er@sunet.se</A>
<BR>
This page was last updated  2007-05-25, 14:43.
        </body>
</html>
Connection to host lost.
```

E-post

E-post var en av de tidiga drivkrafterna för Internets utveckling. Det som först var enkelt och praktiskt, att man kunde nå sin SMTP-server från i stort sett vilken IP-adress som helst, har idag blivit svårt. SMTP-trafik filtreras och stoppas av operatörer och företagsnät. Spam i sig, men även rädslan för att få servrar svartlistade som spamservers, har gjort SMTP-trafiken komplicerad.

Om du väljer att sätta upp SMTP-server via en vanlig ADSL-anslutning kommer det i vanliga fall inte att fungera. Din Internetoperatör stoppar all SMTP-trafik till dig (port 25). En bakgrund till detta är att flera Linuxdistributioner startade en SMTP-server som standard, även om användaren främst tänkte sig servern för ett annat ändamål. Alltså fanns det en mängd e-post servrar som var felaktigt uppsatta. De hade dålig säkerhet och gamla versioner med kända säkerhetshål. Detta utnyttjades av dem som skickade spam och oskyldiga maskiner blev mellanstationer för spam.

Ett problem med SMTP har också varit att säkerheten är låg. Förr kunde man logga in på en SMTP-server och utge sig för att vara en godtycklig avsändare och skicka e-post till vem som helst. Det står i RFC 821 hur man ska göra. Det är fortfarande enkelt att utge sig för att vara någon annan med e-post. (Detta gäller ju faktiskt även vanliga brev.) Så var försiktig med hur du följer instruktioner du fått via e-post.

Det här har man försökt att lösa med att man idag behöver logga in för att få skicka e-post eller att SMTP-servern bara accepterar inkommande post från det lokala nätverk som den sitter på. Om vi använder telnet på port 25 ser vi att inloggning behövs:

```
C:\> telnet smtp.minserver.se 25
220 ironport.bredband.com ESMTP
EHLO mailtest.se
250-ironport.minserver.com
250-8BITMIME
250-SIZE 10485760
250-STARTTLS
250-AUTH PLAIN LOGIN
250 AUTH=PLAIN LOGIN
MAIL FROM: hakan@twoviews.se
250 sender <hakan@twoviews.se> ok
RCPT TO: hakan.lindberg@b3it.se
550 Sorry. SMTP AUTH required.
```

Hantering av e-post kräver ofta två protokoll. SMTP för att skicka e-post, POP eller IMAP för att hämta meddelanden. Detta gör konfigurationen lite svårare men även felsökning. Oftast är användning av POP och IMAP öppen medan SMTP är stängd. Flera varianter finns också på hur säkerheten ska ökas. Till exempel att klienterna förväntas starta med att hämta e-post via POP, som kräver inloggning för att sedan skicka med SMTP.

Ska man göra användning av e-post enkel så är det lättast att använda webbaserad e-post. Tyvärr är inte gränssnitten i webbläsare lika utvecklade.

Ping och traceroute

Det finns ett antal växlar till kommandot ping. Med växeln -l kan man påverka storleken på paketen. Ju längre paketet är desto längre tid tar det att skicka ut paketet. Kommandot är även användbart för att hitta problem med fragmentering och tunnling. Skillnaden i fördröjning och framkomlighet kan vara stor mellan paketlängderna 1460 och 1500 byte. Om en länk mellan server och klient använder tunnling (IP i IP eller IPsec VPN) så tillkommer headerinformation vilket gör att paketen behöver fragmenteras. En lösning är då att ställa ner MTU (Maximum Transmission Unit) på inblandade noder.

Med växlarna -i och -w kan man påverka intervallet mellan varje paket respektive hur lång tid man ska vänta på svaret. Vill man skicka ett flertal paket, ändå tills man avbryter med ctrl-C, lägger man till växeln -t (detta är standard i Linux och Unix).

Ping ger även information om fördröjning och antal routerhopp.

```
C:\>ping www.twoviews.se

Skickar signaler till www.twoviews.se [62.119.28.104] med 32 byte data:

Svar från 62.119.28.104: byte=32 tid=305ms TTL=50
Svar från 62.119.28.104: byte=32 tid=344ms TTL=50
Svar från 62.119.28.104: byte=32 tid=273ms TTL=50
Svar från 62.119.28.104: byte=32 tid=291ms TTL=50

Ping-statistik för 62.119.28.104:
    Paket: Skickade = 4, mottagna = 4, Förlorade = 0 (0 %),
Ungefärligt överföringstid i millisekunder:
    Lägsta = 273 ms, Högsta = 344 ms, Medel = 303 ms
```

Den genomsnittliga fördröjningen ovan är cirka 270 ms vilket är ett normalt värde för en länk via 3G, annars hade vi haft ett värde som varit cirka tio gånger lägre. När vi tog emot paketet hade den TTL = 50. De flesta avsändare sätter TTL till 128, 64 eller 32. Det är alltså rimligen 14 (64–50) routerhopp mellan vår klient och servern. Om vi använder traceroute kan vi verifiera detta.

```
C:\> tracert www.twoviews.se

Spårar väg till www.twoviews.se [62.119.28.104]
över högst 30 hopp:

  1  2445 ms   159 ms   160 ms  10.9.51.1
  2   137 ms   136 ms   159 ms  10.9.51.4
  3   136 ms  1630 ms   461 ms  10.9.50.2
  4   399 ms   488 ms   489 ms  212.181.222.131
  5   546 ms   509 ms   711 ms  vrrx50br2-fe2-0.teliamobile.net [192.36.252.137]
  6   376 ms   400 ms   398 ms  vrrx50ir1-fe2-0.teliamobile.net [192.36.252.214]
  7   402 ms   448 ms   451 ms  10.2.2.1
  8   417 ms   399 ms   419 ms  mobile-vrr.telia.net [192.36.252.198]
  9   354 ms   410 ms   408 ms  vrr-d2.link.se.telia.net [81.228.78.216]
 10   365 ms   459 ms   469 ms  g-ra-c1-link.se.telia.net [81.228.73.80]
 11   404 ms   479 ms   449 ms  g-br-peer1-link.se.telia.net [81.228.73.145]
 12   465 ms     *      493 ms  netnod-ix-ge-b-gbg-4470.utfors.net [195.69.116.66]
 13   348 ms     *      355 ms  ge-0-1-0.se-mlmms001-pe-1.tu.telenor.net [212.105.101.81]
 14   381 ms   469 ms   480 ms  62.119.244.106
 15   387 ms   499 ms   429 ms  www4.aname.net [62.119.28.104]

Spårning utförd.
```

Kommandot traceroute ger även värdefull information om hur trafiken kommer fram. Programmet gör även en baklängesuppslagning av de routrar som är inblandade och namnet ger en vägledning. Vi kan se att trafiken går via Telia Mobile via Internetknutpunkten (Netnod IX) till Telenors nät (vi ser rester av att Telenor köpt Utfors). Och vi ser att www.twoviews.se verkar ligga på ett webbhotell.

Referenser

Practical TCP/IP	Niall Mansfield Addison-Wesley 2003
How to troubleshoot TCP/IP connectivity with Windows XP	Microsoft, artikel-id 314067 (artikeln tar upp ett par aspekter som ej behandlats i detta kapitel)